09/553301 PCT/EP 99/07026

BUNDESREPUBLIK DEUTSCHLAND

EJV

EP99/7026

14. 10. 1999

(70)

Bescheinigung

Die Philips Patentverwaltung GmbH in Hamburg/Deutschland hat eine Patentanmeldung unter der Bezeichnung

"Steuereinheit zum Schutz von integrierten Schaltungsteilen vor 'Differential Power Analysis' "

am 30. September 1998 beim Deutschen Patent- und Markenamt eingereicht.

Die angehefteten Stücke sind eine richtige und genaue Wiedergabe der ursprünglichen Unterlagen dieser Patentanmeldung.

Die Anmeldung hat im Deutschen Patent- und Markenamt vorläufig das Symbol G 06 F 12/14 der Internationalen Patentklassifikation erhalten.

München, den 30. September 1999

Deutsches Patent- und Markenamt

Der Präsident

Im Auftrag

Hiebinger

Aktenzeichen: 198 44 992.5

A 9161
06 90
11/98

Steuereinheit zum Schutz von integrierten Schaltungsteilen vor 'Differential Power Analysis'

Die 'Differential Power Analysis' ist eine neue Methode, welche es erlaubt, über die reine Funktionalität hinaus zusätzliche interne Informationen einer integrierten Schaltung zu gewinnen. Abbildungen 1 und 2 zeigen die Anordnung einer integrierten Schaltung (1), welche insbesondere mit zwei Operandenregistern (5 und 6) ausgestattet ist, eines Registers (2) und der Steuereinheit (3) selbst. Das gesamte Konzept ist Gegenstand dieser Erfindung.

Die 'Differential Power Analysis' hat den Ansatz, daß neben den Ein-/Ausgangssignalen zusätzlich die Stromaufnahme (a) beziehungsweise Spannungseinbrüche an der Versorgungsspannung (b) der integrierten Schaltung analysiert werden. Der Erfolg dieser Analysemethode hängt davon ab, ob man eine Anzahl A von analogen (a oder b) Signalverläufen S(k,t) über die Zeit t mit k={1,...,A} unterschiedlichen Operanden so aufnehmen kann, daß eine Summenbildung der Form

$$T(i,t) = \sum_{k=1}^{A} p(i,k) \cdot S(k,t) \qquad \text{mit den Koeffizienten } p(i,k),\ i=\{0,1,2,\ldots\}$$

möglich ist. Betrachtet man unterschiedliche Signalverläufe $S(k_1,t_1)$, $S(k_2,t_1)$, $S(k_3,t_1)$, ... zum gleichen Zeitpunkt $t=t_1$, kann eine 'Differential Power Analysis' nur funktionieren, wenn die integrierte Schaltung in diesem Moment die gleiche Rechenoperation ausführt mit unterschiedlichen Operanden k={1,...,A}, d.h. die Signalverläufe S(k,t) müssen genau übereinandergelegt werden können. Dieses gilt nicht nur für die Berechnung selbst, sondern auch für die Ein- und Ausgabe von Daten.

Die vorliegende Erfindung verschleiert die Zeitbereiche, sowohl die der eigentlichen Berechnungen als auch die der Datenein- und Datenausgabe. Bei geeigneter Ansteuerung des Registers (2) kann nicht mehr festgestellt werden, wann eine wirkliche Berechnung oder Ein-/Ausgabe stattfindet. Die 'Differential Power Analysis' wird so erheblich erschwert.

Die integrierte Schaltung ist mit zwei Operandenregistern ausgestattet (Abbildung 2). Diese erlauben die Ein- und Ausgabe von Daten über Operanden Register 1 (5) auch während die Recheneinheit aktiv ist via Operanden Register 2 (6).

Abbildung 3 zeigt den zeitlichen Verlauf einer herkömmlichen Berechnung mit vor- und nachgeschalteten Ein- und Ausgabephasen. Bei der 'Differential Power Analysis' können die Phasen der Berechnungen und Ein-/Ausgabe leicht identifiziert werden, insbesondere welche Eingaben bei einer Berechnung Verwendung finden und welche Ausgaben die Folge sind.

In Abbildung 4 ist gezeigt, wie die Berechnungen sowie die Ein-/Ausgaben verschleiert werden können mit Hilfe einer speziellen Steuereinheit, welche den Datenfluß der beiden Operandenregister (5) und (6) steuert. Berechnungen finden immer statt (Abbildung 4). Ob aber eine Berechnung von der Eingabe abhängt oder eine Ausgabe liefert, wird bestimmt durch die Kopieroperationen R1-2 (Eingabe: kopiere Registerinhalt 1 nach 2) und R2-1 (Ausgabe: kopiere Registerinhalt 2 nach 1). Die Berechnungen vor R1-2 bzw. nach R2-1 können Dummy-Berechnungen sein. Zusätzliche (Dummy-) Ein- und Ausgaben können während der Berechnung stattfinden. Sowohl die Dummy-Berechnungen als auch die Dummy-Ein/ausgaben erzeugen Strom- bzw. Spannungsänderungen, welche denen der wirklichen Berechnungen und Ein-/Ausgaben sehr ähnlich sind.

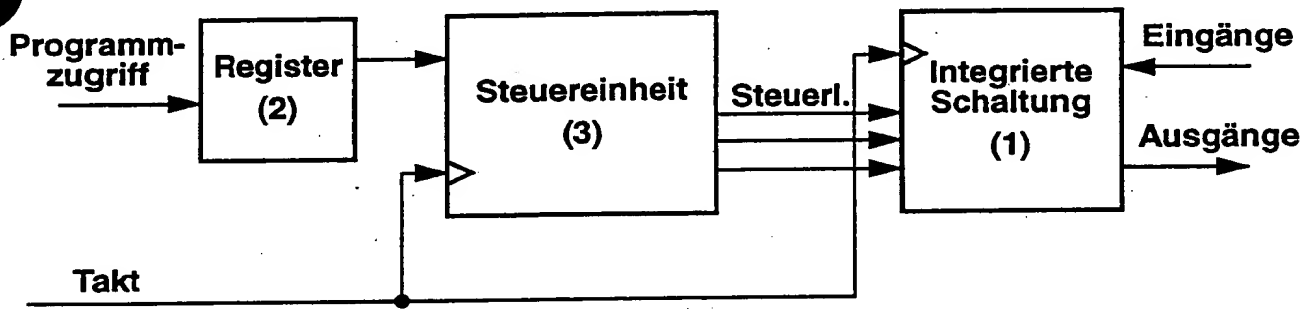

Abbildung 1: Steuereinheit

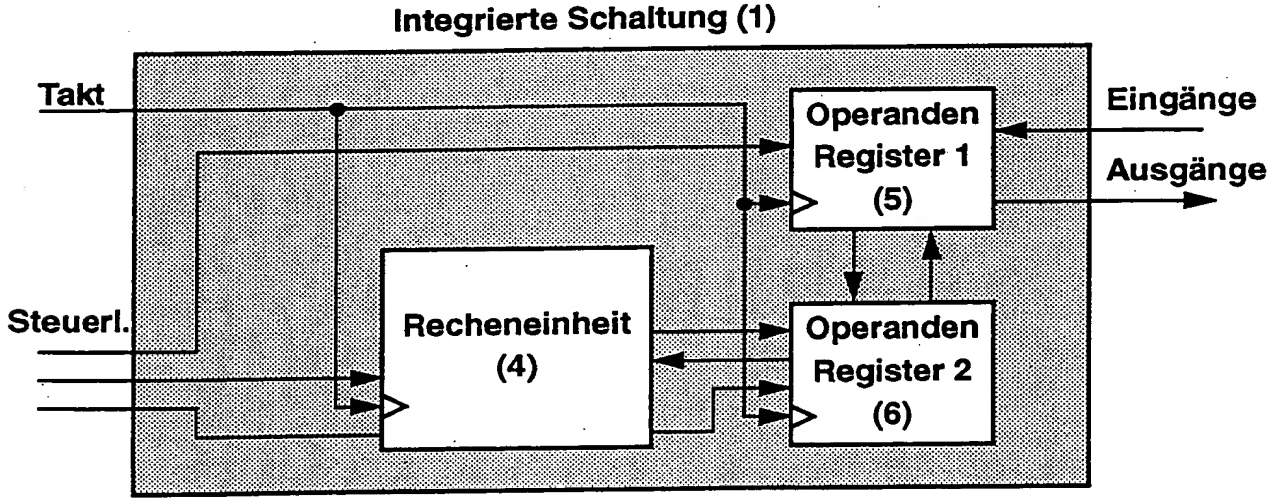

Abbildung 2: Operanden Register

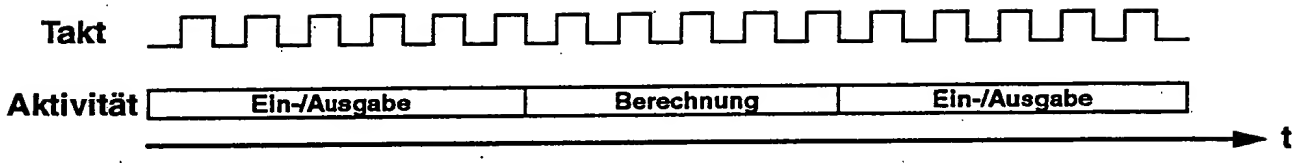

Abbildung 3: Betrieb ohne Steuereinheit

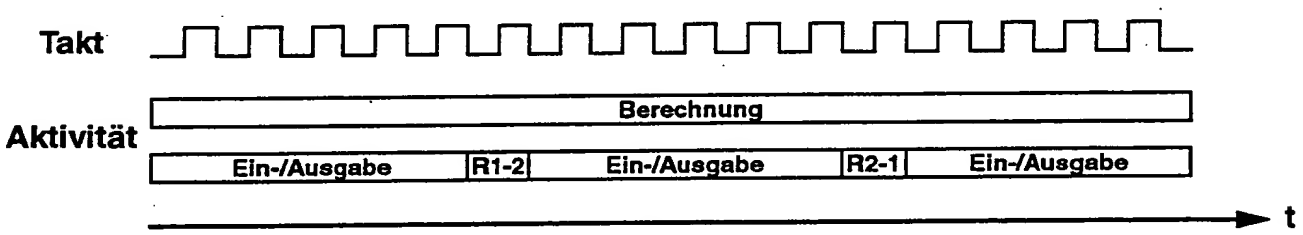

Abbildung 4: Betrieb mit Steuereinheit

Die vorliegende Erfindung, die eine Steuereinheit zum Schutz von integrierten Schaltungsteilen vor einem Eingriff mit Hilfe der sogenannten „Differential Power Analysis" (DPA) zum Gegenstand hat, zielt speziell auf die Ein- und Ausgabephasen einer in den integrierten Schaltungsteilen mit Hilfe digitaler, elektronischer Signalverarbeitung durchzuführenden Berechnung ab, da auch Ein- und Ausgaben anhand des Stromverbrauchs mit Hilfe der DPA analysiert werden können. Entsprechend ist bei der DPA von Interesse, wann eine Berechnung beginnt oder endet. Genau diese Informationen werden im Stromverbrauchssignal unterdrückt.